NEWS theJohnsonian

April 13, 2016

Police Blotter

Bus Stop Assault
4/8/16

Officers were stopped in Wofford Parking Lot by a student in reference to an assault that had happened in Dinkins parking lot. According to the student, the victim and the two subjects we're on their way back from a club in Charlotte on a party bus, the victim had an argument with the two subjects. After the argument, everything calmed down until they arrived back on campus. The subjects exited in front of the victim and was attacked by the two subjects. The student tried to intervene but was pushed to the ground by the subjects. The student said that one of the subjects was choking the victim and forcing him to the ground. The victim got out of the choke, but was then kicked in the head.

The officers then made contact with the victim, while other officers found the first subject outside of the Dalton building, where he tried to flee but was apprehended. According to the victim, the first subject also punched him in the mouth. The subject was placed under arrest for assault and battery and was sent to the Rock Hill Law center for booking.

Officers could not locate the second subject, but a warrant for his arrest has been issued.

Dine and Dash
4/4/16

Winthrop Police Chief Zebedis noticed the subject riding a green bike on Alumni Drive carrying two large sacks. When asked about the sacks, the subject stated that they were his laundry that he had taken from the laundromat on Cherry Road. As Zebedis walked towards the subject, the subject attempted to conceal the sacks under his jackets that he was carrying.

Upon further questioning and asking to see his laundry, the subject stated that he found the sacks outside of a building and just took them. Upon opening the sack, police found a box of ground beef patties, a box of skinless boneless pangasius, a box of sliced bacon, a box of pork sausage and a box of shrimp.

Upon speaking with Aramark, the food was confirmed to be a shipment for campus, and the subject admitted to taking the foods without paying for it nor asking permission. The subject was placed under arrest for petty larceny.

A new twist on career fairs

Jacob Hallex/ The Johnsonian

Students and local business professionals gathered in the Richardson Ballroom for a reverse career fair. Students sold themselves to potential employers by presenting posters about their work.

CAREER • from front

The Center for Career and Civic Engagement teamed up with the office of Student Activities for a reverse career fair in Richardson Ballroom, where student leaders had the chance to stand on the other side of the table and showcase their leadership, internship, event planning, professional or service project experiences to employers.

"We are excited to have 27 students here today to showcase their talents," said Meagan McMullen the Career and Serve Learning Consultant at Winthrop. "This is a great chance for our employers to see how multifaceted our students are."

Student participants were spotted handing out business cards as they proudly explained the various goals and objectives of their brands or projects.

"My brand is an extension of me," said Joseph Ferguson a senior political science major. "So my display has everything I have been doing over the past four years on it."

Ferguson took the time and used the platform created at the career fair to craft his content, while making himself all-around marketable.

All 27 of the students were required to meet one-on-one sessions with a career counselor at the Center for Career and Civic Engagement Center to polish their resumes, create the displays or business cards and elevator speeches for employers to see.

After a month of preparation and once the display materials were approved prior to the fair, participants became eligible for funding to cover any costs for resumes and displays.

"This is like my little baby and I am proud of the work I have been able to do over these past four years to help my brand in the future," said Ferguson.

The display boards gave the students the chance to visually show their resumes without a sheet of paper.

"This is a creative way for me to show my resume," said Faith Holmes junior mass communication major.

All undergraduate students were given the chance to apply to showcase their work.

The truth about digital intelligence gathering

How much information is out there on you and how can it be used without your knowledge?

Thomas Calamia
calamiat@mytjnow.com

We live in a new and completely digital age. Technology within the past few years has advanced exponentially.

In this time of such quick advancement, little do we know that we are slowly giving up more and more of our own personal information to different entities: such as the government and private corporations.

Alluded to in the Fourth Amendment of the Constitution, each of us is guaranteed a right to privacy. It gives us the right "to be secure in their persons, houses, papers, and effects" against "unwarranted search and seizure."

This means that without the necessary warrants, the government cannot gather information on a person without a probable cause of a crime. However, things become a little hazier when digital information is involved.

"It is not at all clear if there is a general consensus about what people think about privacy and security, and it's largely due to the fact that terms are not well defined," said Jeffrey Vagle Digital and Privacy law professor at the University of Pennsylvania Law School. "There is not good one definition of privacy."

Unlike technology, the law is not so quick to adapt. With how our government works, it usually takes a considerable amount of time to get a bill signed into law. Since technology is always evolving and advancing, this makes governing technology and communication difficult.

"We're not going to be changing that, certainly not without a constitutional amendment," Vagle said. "There is nothing technologically specific in that amendment, but we've had to adopt that amendment based on changes in technology. So it's not so much changing the law, new laws do get written from time to time, but it's changing the way we think about the law with these new technologies and how we use them."

With more and more people flocking to the internet and using technology such as smart phones, we are willingly giving up personal identifiable information, or PII.

The ability to send messages, receive email, interact with social media, view and perform banking information from our smart phones all require individuals to willingly give up that information. These are done by contracts, sometime 10 page blocks of text that we sign away without a second thought every day: Terms of Service agreements.

With these contracts, we willingly give these companies our information and in exchange they can keep our information safe. This, in theory, should keep our information safe.

However, if the government requires information on an individual backed by a warrant and probable cause, the government can ask for access to that information. Most companies are actually very willing to give that information up as well, even if they are not presented with a warrant.

In the book, "The Digital Person: Technology and Privacy in the Information Age," by Daniel J. Solove, he recites an example of how Northwest Airlines secretly turned over to NASA its customer data—including addresses, phone numbers, and credit card information—for use in a government data mining project.

"In a December 2008 survey of nearly 800 chief security officers, almost 25 percent said that they would supply information to the government without a court order, with 41 percent doing so in cases involving national security," he said.

However, this information stored on company servers can be breached. Like in the Sony and Target hacks, where individuals PII and banking information was stolen, there is little that can be done after the fact.

To make sure that this doesn't happen, companies have partnered with both the Department of Homeland Security and other companies called Data Insurance companies.

"One of the key reasons businesses need to consider a cyber insurance policy or endorsement is that general liability coverage only covers losses related to a physical act, such as a person breaking into an office and stealing files or computers," said Keith Kirkpatrick in a Communications of The ACM.

As of now, the best way to protect your PII is to be more careful with what you tell people.

Once data is out there, it is out there. In Kirkpatrick's article, Christine Marciano president of Cyber Data-Risk Managers LLC, a Princeton, NJ-based cyber-insurance broker suggest using good "cyber hygiene."

Marciano defines cyber hygiene as, "implementing and enforcing data security and privacy policies, procedures, and controls to help minimize potential damages and reduce the chances of a data security breach."

Thomas Calamia | News Editor
calamiat@mytjnow.com